LISTING OF THE CLAIMS PER 37 C.F.R. §1.121

1-174. (Cancelled)

175. (Currently Amended) A method of redirecting data items from a messaging host system to a user's mobile device, comprising:

establishing a secure communications link between a computer system associated with the user and the user's mobile device;

sending a first encryption key, which is generated at [[from]] the computer system associated with the user in dependence on the user's interaction therewith, to the redirector host system;

storing the first encryption key at the redirector host system;

sending a first decryption key from the computer system associated with the user to the user's mobile device using the secure communications link;

detecting a new data item for the user at the messaging host system by the redirector host system;

determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

if the new data item should be redirected, then encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

transmitting the encrypted new data item from the redirector host system to the user's mobile device.

176. (Previously Presented) The method as recited in claim 175, wherein establishing a secure communications link between the computer system associated with the user and the user's mobile device further comprises establishing a serial connection between the computer system associated with the user and the user's mobile device.

177. (Previously Presented) The method as recited in claim 175, wherein establishing a secure communications link between the computer system associated with the user and the user's mobile device further comprises using Secure Sockets Layer (SSL) protocol.

178. (Previously Presented) The method as recited in claim 175, wherein sending the first encryption key and sending the first decryption key further comprise generating a shared key.

179. (Previously Presented) The method as recited in claim 175, further comprising generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

180. (Previously Presented) The method as recited in claim 175, wherein sending the first encryption key further comprises generating a public key.

181. (Previously Presented) The method as recited in claim 180, wherein sending the first decryption key further comprises generating a private key.

182-183. (Cancelled)

184. (Previously Presented) The method as recited in claim 175 further comprising:

sending a second decryption key from a computer system associated with the user to the redirector host system;

storing the second decryption key at the redirector host system; and

sending a second encryption key from the computer system associated with the user to the user's mobile device using the secure communications link.

185. (Previously Presented) The method as recited in claim 184, wherein sending the second encryption key and sending the second decryption key further comprise generating a shared key.

186. (Previously Presented) The method as recited in claim 184, wherein sending the second encryption key and sending the second decryption key further comprises generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

187. (Previously Presented) The method as recited in claim 184, wherein the sending the second encryption key further comprises generating a public key.

188. (Previously Presented) The method as recited in claim 187, wherein the sending the second decryption key further comprises generating a private key.

189. (Cancelled)

190. (Previously Presented) The method as recited in claim 184 further comprising:

receiving an encrypted data item from the user's mobile device at the redirector host system; and

decrypting the encrypted data item to recover the data item.

191. (Previously Presented) The method as recited in claim 190 further comprising the step of transmitting the data item to a destination system using an electronic address associated with the user at the messaging host system, wherein data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

192. (Currently Amended) A system for redirecting data items from a messaging host system to a user's mobile device, comprising:

a redirector host system operable to be connected to the messaging host system;

means for establishing a secure communications link between a computer system associated with the user and the user's mobile device;

means for sending a first encryption key, which is generated at [[from]] the computer system associated with the user in dependence on the user's interaction therewith, to the redirector host system;

means for storing the first encryption key at the redirector host system;

means for sending a first decryption key from the computer system associated with the user to the user's mobile device using the secure communications link;

means for detecting a new data item for the user at the messaging host system by the redirector host system;

means for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

means for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

means for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

193. (Previously Presented) The system as recited in claim 192, wherein the means for establishing a secure communications link between the computer system associated withe the user and the user's mobile device further comprises a serial connection between the computer system associated with the user and the user's mobile device.

194. (Previously Presented) The system as recited in claim 192, wherein the means for establishing a secure communications link between the computer system associated with the user and the user's mobile device further comprises means for using Secure Sockets Layer (SSL) protocol.

195. (Previously Presented) The system as recited in claim 192, wherein the means for sending the first encryption key and the means for sending the first decryption key further comprise means for generating a shared key.

196. (Previously Presented) The system as recited in claim 192, wherein the means for ~~a~~ sending the first encryption key and the means for sending the first decryption key further comprise means for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

197. (Previously Presented) The system as recited in claim 192, wherein the means for sending the first encryption key further comprises means for generating a public key.

198. (Previously Presented) The system as recited in claim 197, wherein the means for sending the first decryption key further comprises means for generating a private key.

199-200. (Cancelled)

201. (Previously Presented) The system as recited in claim 192 further comprising:

means for sending a second decryption key from a computer system associated with a second user to the redirector host system;

means for storing the second decryption key at the redirector host system; and

means for sending a second encryption key from the computer system associated with the user to the user's mobile device using the secure communications link.

202. (Previously Presented) The system as recited in claim 201, wherein the means for sending the second encryption key and the means for sending the second decryption key further comprise means for generating a shared key.

203. (Previously Presented) The system as recited in claim 201, wherein the means for sending the second encryption key and the means for sending the second decryption key further comprise means for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

204. (Previously Presented) The system as recited in claim 201, wherein the means for a second encryption key further comprises means for generating a public key.

205. (Previously Presented) The system as recited in claim 204, wherein the means for sending the second decryption key further comprises means for generating a private key.

206. (Cancelled)

207. (Previously Presented) The system as recited in claim 201 further comprising:

means for receiving an encrypted data item from the user's mobile device at the redirector host system; and

means for decrypting the encrypted data item using the second decryption key to recover the data item.

208. (Previously Presented) The system as recited in claim 207 further comprising the means for transmitting the data item to a destination system using an electronic address associated with the user at the messaging host system, wherein data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

209. (Previously Presented) A computer-accessible medium having a sequence of instructions which, when executed by a processing entity, effectuate redirection of data items from a messaging host system to a user's mobile device, the computer-accessible medium comprising:

instructions for establishing a secure communications link between a computer system associated with the user and the user's mobile device;

instructions for sending a first encryption key, which is generated at [[from]] a computer system associated with the user in dependence on the user's interaction therewith, to the redirector host system;

instructions for storing the first encryption key at the redirector host system;

instructions for sending a first decryption key from the computer system associated with the user to the user's mobile device using the secure communications link;

instructions for detecting a new data item for the user at the messaging host system by the redirector host system;

instructions for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

instructions for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

instructions for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

210. (Previously Presented) The computer-accessible medium as recited in claim 209, wherein the instructions for establishing a secure communications link between computer system associated with the user and the user's mobile device further comprises instructions for establishing a serial connection between the computer system associated with the user and the user's mobile device.

211. (Previously Presented) The computer-accessible medium as recited in claim 209, wherein the instructions for establishing a secure communications link between the computer system associated with the user and the user's mobile device further comprises instructions for using Secure Sockets Layer (SSL) protocol.

212. (Previously Presented) The computer-accessible medium as recited in claim 209, wherein the instructions for sending the first encryption key and for sending the first decryption key further comprise instructions for generating a shared key.

213. (Previously Presented) The computer-accessible medium as recited in claim 209, wherein the instructions for sending the first encryption key and for sending the first decryption key further comprise instructions for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

214. (Previously Presented) The computer-accessible medium as recited in claim 209, wherein the instructions for sending a first encryption key further comprises instructions for generating a public key.

215. (Previously Presented) The computer-accessible medium as recited in claim 214, wherein the instructions for sending a first decryption key further comprises instructions for generating a private key.

216-217. (Cancelled)

218. (Previously Presented) The computer-accessible medium as recited in claim 209 further comprising:

instructions for sending a second decryption key from the computer system associated with the user to the redirector host system;

instructions for storing the second decryption key at the redirector host system; and

instructions for sending a second encryption key from the computer system associated with the user to the user's mobile device using the secure communications link.

219. (Previously Presented) The computer-accessible medium as recited in claim 218, wherein the instructions for sending the second encryption key and for sending the second decryption key further comprise a code portion for generating a shared key.

220. (Previously Presented) The computer-accessible medium as recited in claim 218, wherein the instructions for sending the second encryption key and for sending the second decryption key further comprise instructions for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

221. (Previously Presented) The computer-accessible medium as recited in claim 218, wherein the instructions for sending the second encryption key further comprises instructions for generating a public key.

222. (Previously Presented) The computer-accessible medium as recited in claim 221, wherein the instructions for sending the second decryption key further comprises instructions for generating a private key.

223. (Cancelled)

224. (Previously Presented) The computer-accessible medium as recited in claim 218 further comprising:

instructions for receiving an encrypted data item from the user's mobile device at the redirector host system; and

instructions for decrypting the encrypted data item to recover the data item.

225. (Previously Presented) The computer-accessible medium as recited in claim 224 further comprising instructions for transmitting the data item to a destination system using an electronic address associated with the user at the messaging host system, wherein data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.